UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

CHRISTOPHER GEORGE PABLE, **Plaintiff,** **v.** **CHICAGO TRANSIT AUTHORITY and CLEVER DEVICES LTD.,** **Defendants.**	**Case No. 1:19-cv-7868** **Judge Elaine E. Bucklo** **Mag. Judge Heather K. McShain**
CHICAGO TRANSIT AUTHORITY, **Counter-Plaintiff,** **v.** **CHRISTOPHER GEORGE PABLE,** **Counter-Defendant.**	

PABLE'S OPPOSITION TO CTA'S MOTION TO COMPEL

The CTA's motion to compel should be denied. Mr. Pable has provided all relevant information from his cell phone, and has not withheld any relevant information regarding his website. The CTA's arguments to the contrary are based on misconstrued facts, unfounded accusations, and a deliberate indifference to the actual issues in this case.

BACKGROUND

The Parties' Claims

While employed by the CTA as a computer programmer and analyst, Mr. Pable discovered a "Skeleton Key" in the CTA's BusTime system, a software product provided to the CTA by Clever Devices and used to provide information and alerts regarding the status of CTA buses. (Complaint at ¶¶ 29-34 (Dkt. #1)) This Skelton Key posed a security risk to the CTA: It was easily accessible over unencrypted network traffic generated by the BusTime system and, if obtained by someone intent on mischief or worse, could be used to gain complete access to the system and, among other things, broadcast alerts and messages to the public and otherwise disrupt transit system operations. (*Id.* at ¶¶ 35-36)

Mr. Pable reported his discovery to his supervisor, Mr. Haynes, who decided (over Mr. Pable's objection) to test the Skeleton Key found in the CTA's system on another transit system to determine whether this was an issue with only the CTA's BusTime system or with BusTime systems more generally, which could pose security risks for many transit systems around the world. (*Id.* at ¶¶ 37-39) Mr. Haynes used the Skeleton Key to post and immediately remove an alert that has previously been issued on Dayton, Ohio's BusTime system. Unbeknownst to Mr. Haynes (or Mr. Pable), Dayton's system was configured to post its alerts on its Twitter account, so the alert, which otherwise would have briefly appeared and disappeared on Dayton's website, for example, was broadcast to the public via Twitter, who were told, for the second time, that a certain bridge was out due to construction, which was still true at the time of the test. (*Id* at ¶ 40)

Mr. Haynes proceeded to test the Skeleton Key on a number of other BusTime systems, though in a manner that did not post any alerts, and found that the Skeleton Key allowed him to access many BusTime systems. (*Id.* at ¶ 41) After apologizing to Dayton (whose personnel were

surprised but acknowledged Mr. Haynes had done no harm and, in fact, appreciated the value of the information he obtained via the test), Mr. Haynes notified Clever Devices of the existence of the Skeleton Key. (*Id.* at ¶¶ 42-45) Clever Devices expressed no gratitude to Mr. Haynes, but rather focused on its displeasure that he had used the Skeleton Key to access other agencies' BusTime systems. (*Id.* at ¶ 46) Nonetheless, Clever Devices acknowledged the risk posed by the Skeleton Key by issuing a security alert to its BusTime clients and took steps to disable the Skeleton Key in the CTA's and other BusTime systems. (*Id.* at ¶¶ 47-48) Mr. Haynes notified several other CTA employees of this issue while it was unfolding, and his supervisor, Mr. Psomos, soon after the issue was resolved with Dayton and Clever Devices. All of this occurred between August 17th and August 24th in 2018. (*Id.* at ¶ 52)

Mr. Haynes and Mr. Pable thought the matter resolved. But on October 22, 2018, Clever Devices sent a letter to Dorval Carter, President of the CTA, alleging that in conducting the Dayton test, Mr. Haynes, and Mr. Pable, had violated the licensing agreement in place between the CTA and Clever Devices and stating that their actions were "likely" in violation of unspecified federal and state laws as well. (*Id.* at ¶¶ 53-55) Within less than 24 hours after Mr. Carter received Clever Devices's letter, Mr. Haynes and Mr. Pable were put on leave, their access to CTA's premises and systems disabled, and – relevant to the CTA's motion here – the CTA disabled the profile on Mr. Pable's phone under which substantially all of his work-related communications and applications had been installed, effectively preventing him (or anyone else) from accessing this data. (*Id.* at ¶ 56; CTA Motion Exs. B & K) Among the data rendered inaccessible by the CTA's action was a password manager that Mr. Pable had been using to store his password to access his CTA computer that would allow access to his encrypted hard drive via his thumbprint. (CTA Motion Ex. B)

Following an "investigation" by the CTA, Mr. Pable was forced to resign or face termination on November 8, 2021. He chose the former. (Complaint at ¶¶ 55-59) He filed a Complaint under the Public Transportation Employee Protections provision, 6 U.S.C. § 1142, of the National Transit Systems Security Act ("NTSSA") with the Department of Labor on May 2, 2019 and, after the expiration of the statutory period for disposition of his claim without any action by the Department, filed this case on December 2, 2019. (*Id.* at ¶¶ 18-21)

On August 3, 2020, the CTA filed a counterclaim against Mr. Pable, alleging that his encryption of the hard drive on his CTA computer and his alleged implantation of some sort of "self destruct" mechanism that he could trigger, or that would somehow be triggered after his termination, violated the Computer Fraud and Abuse Act and caused damage to the CTA in the form of having to retain a forensic expert to access the drive for discovery purposes.[1]

Among the affirmative defenses asserted by the CTA is the assertion that it would have fired Mr. Pable even if he had not reported the existence of the Skeleton Key (Answer and Affirmative Defenses at pp. 27-28 (Dkt. # 8)),[2] and that the misconduct alleged in its counterclaim precludes his claim under the doctrines of "unclean hands" and "after acquired evidence." (Additional Affirmative Defenses at pp. 1-2 (Dkt. # 30))[3]

---

[1] The Court should know that the viability of the CTA's counterclaim under the Computer Fraud and Abuse Act may well be impacted by a case currently pending at the U.S. Supreme Court. *See Van Buren v. United States*, Dkt. # 19-783 (S.Ct. argued Nov. 30, 2020) (considering whether the Act applies to employees authorized to use a computer who nonetheless use the computer for an allegedly impermissible purpose).

[2] The statutorily mandated standard for Mr. Pable's claim requires only that he show his reporting of the Skelton Key "was a contributing factor" in his termination; the defendants may only defeat such a claim if they "demonstrate[], by clear and convincing evidence, that the employer would have taken the same unfavorable personnel action in the absence of" Mr. Pable's report. 6 U.S.C. §1142(c)(2)(B) & (c)(7).

[3] Any application of an "unclean hands" defense, which is an equitable doctrine, is precluded here by the specific standard articulated in the statute under which Mr. Pable's claim arises, and in any

Relevant Discovery

The CTA requested, and Mr Pable was obviously obliged to produce, any communications relevant to the case. The parties agreed on a list of search terms to be applied to electronic information to capture relevant items and a time period for which such data would be searched. In addition to application of these parameters to his personal email and other cloud-based accounts, the CTA's requested, and Mr. Pable undertook, the application of the same to the cell phone he used during the relevant period of time. Counsel for Mr. Pable retained a forensic expert to image, search, and facilitate the production of the results of this work.

As a result of the foregoing work, Mr. Pable produced the following on July 30, 2020:

- 192 email messages from his personal Gmail account in their native .eml format along with pdf print outs of the same spanning 1,177 pages;
- An Excel spreadsheet containing the content and metadata of 2032 messages retrieved from his Google Hangouts account, along with 23 images and 2 video files associated therewith;
- 25 screen shots of his cell phone showing multiple messages accessed via Google Hangouts, thus reflecting the "real world" look and feel of the messages reflected on the spreadsheet that were accessible from his cell phone at the time of its forensic examination, plus related images sufficient to identify the relevant conversation threads, the parties to the conversations, and the times the messages were sent;
- 31 screen shots of his cell phone showing multiple messages accessed via Signal, thus reflecting the "real world" look and feel of the messages accessible from his cell phone at the time of its forensic examination, plus related images sufficient to identify the related conversation threads, the parties to the conversations, and the times the messages were sent

---

event is not applicable in the context of a legal claim for violation of a public-policy based statute protecting whistleblowers. *See generally*, *Scheiber v. Dolby Laboratories, Inc.*, 293 F.3d 1014 (7th Cir. 2002). Similarly, there is no potential for the application of the "after-acquired evidence" doctrine where, as here, the statute includes a provision allowing a showing the employer would have acted the same regardless of the protected activity, and the courts have rejected the argument that the doctrine can be used to preclude recovery against employers who violate public-policy based statutes. *See generally*, *McKennon v. Nashville Banner Pub. Co.*, 513 U.S. 352 (1995).

On November 24, 2020, Mr. Pable produced an additional 19 emails from his personal Gmail account in native format and as .pdf files spanning an additional 500 pages as a result of expanding the date range for searches at the request of the CTA, as well as a spreadsheet reflecting the content and available metadata for approximately 150 messages retrieved from his LinkedIn account. On December 22, 2020, Mr. Pable produced the metadata and pdf printouts of an additional 18 messages (some of which contain extensive conversations) from his Google Voice account for both the original and expanded date range.

Mr. Pable's Cell Phone

On October 31, 2020, Mr. Pable produced copies of the two images that were taken of his cell phone. Not surprisingly, these images did not contain large amounts of data. (*See* CTA Motion Ex. J) As counsel for Mr. Pable explained to counsel for the CTA, this is because most of the data (and especially substantially all relevant data) was wiped from the phone when the CTA disabled Mr. Pable's work profile on the device in late October 2018. (CTA Motion Ex. K) Mr. Pable's expert was, however, able to use the phone to retrieve a significant number of Google Hangouts messages and images (which were also retrievable, and had been retrieved and produced from the cloud) and Signal messages (which are not otherwise retrievable and typically not retrievable at all, as Signal is often configured not store messages). (*Id.*)

Mr. Pable's Website

On October 29, 2020, the CTA requested that Mr. Pable produce, "[c]omplete and accurate copies of the archived Websites showing the Websites as they appeared from May 1, 2018 to the present." (CTA Motion Ex. L) Mr. Pable objected to this request on November 13, 2020. (CTA Motion Ex. M). On November 20, 2020, the CTA produced a number of printed pages of material it found on the Internet reflecting material that had been posted or linked to on the site. On

November 29, 2020, counsel for Mr. Pable explained to counsel for the CTA that Mr. Pable does not have any "archives" of his website, and if forced to try to reconstruct its appearance would simply do what the CTA had already done in searching and retrieving historical versions of the website accessible on the Internet. (CTA Motion Ex. K) In addition, counsel for Mr. Pable informed counsel for the CTA that the alleged "proprietary" CTA code supposedly published on Mr. Pable's website was, in fact, a linked to a third-party site hosting this code with the knowledge, and for the benefit, of the CTA to fulfill a requirement that this code be accessible. (*Id.*)

The CTA's Motion

Skeptical of Mr. Pable's representations that there is no additional relevant data available on his cell phone and his representation that he does not have archived copies of his website, the CTA has filed the instant motion to compel.

ARGUMENT

I. Mr. Pable Should Not Be Required to Produce His Cell Phone to the CTA.

As the CTA's own authority provides, "A forensic ESI exam constitutes an extraordinary remedy that is required only if the moving party can actually prove that the responding party has concealed information or lacks the expertise necessary to search and retrieve all relevant data." *Belcastro v. United Airlines, Inc.*, 2019 WL 7049914 at *2 (N.D. Ill. Dec. 23, 2019) (internal quotations omitted). While the Court in *Belcastro* did order the inspection, in that case the phone at issue was central to the conduct at issue (which centered around a picture taken on the phone), and the plaintiff had not retained a professional to search for and extract data from his phone. *Id.* at *3-4. No such circumstances obtain here.

The CTA claims it "knows" additional, unproduced communications exist. (CTA Motion at 14) But the sole foundation for this bold statement is a reference to a text in an August 24, 2018

email from Mr. Haynes to Mr. Pable, which gives no indication of the content of the alleged text. (*Id.* at 8 n.3) Neither Mr. Haynes nor Mr. Pable's productions contain any text from this date, nor has the CTA laid any foundation with either individual as to what the email referred to or what communications they might have had via text (or otherwise). The implication that there existed a text that neither Mr. Haynes nor Mr. Pable retained on their respective phones (even putting aside that any copy on Mr. Pable's phone may have been deleted by the CTA) is hardly a basis for ordering a reexamination of Mr. Pable's device, particularly in light of any evidence that this particular text was both relevant and somehow improperly withheld from the CTA.

The CTA also points to unspecified discrepancies between the text messages produced by Mr. Haynes and Mr. Pable. (CTA Motion at 14) This is neither surprising nor probative. If anything, it shows that the CTA has not only received Mr. Pable's assurances that all accessible communications have been produced, but that it has already received a "check" on this assurance via discovery of Mr. Haynes. And despite claiming there are material discrepancies between the two productions, it has not identified anything specific that supports the claim that Mr. Pable has withheld relevant data.

The CTA also claims it needs to examine Mr. Pable's phone for purposes of proving its counterclaim regarding encryption of Mr. Pable's hard drive. But what it fails to tell the Court is that Mr. Pable has admitted to encrypting the hard drive (pursuant to CTA policy), and to using a program on his phone that, if deleted, would prevent anyone from gaining ready access to the encrypted drive. (Pable Answer at 5 (Dkt. # 34) ("Pable admits he encrypted the Primary Drive of the CTA Computer.") & CTA Motion at Ex. K) (admitting Pable configured his access to the drive via an app since deleted from his phone by the CTA). Assuming it is not legally precluded as a result of the fact that Pable was an authorized user of his computer, the only truly disputed

issues with the respect to the CTA's counterclaim are the propriety of his actions and potentially the damage, if any, to the CTA. No further examination of Mr. Pable's cell phone is at all likely to yield additional information relevant to adjudicating this claim.

The CTA's final argument in support of its motion to compel production of Mr. Pable's phone is its claim that the image provided to the CTA "is compromised or incomplete." (CTA Motion at 16-18) As an initial matter, this argument confuses the aim of discovery. This is not a case about phone images. There is no entitlement or relevance of any image of Mr. Pable's phone. The point is the discovery of relevant communications.

Contrary to the CTA's claim that Mr. Pable "has failed in his obligation to search [for] and produce relevant information, including communications, like text messages and messages sent via either Google Hangouts or Signal" (CTA Motion at 16), Mr. Pable has produced hundreds of pages worth of precisely such messages retrieved from the cloud and ***retrieved from his phone***, as the screen shots (one of which the CTA includes in the body of its motion) obviously demonstrate. Suspicious that Mr. Pable had not produced all relevant messages, the CTA sought to double check his efforts by examining the image taken of Mr. Pable's phone – over Mr. Pable's objection that this was not likely to be helpful. There is no dispute that the image does not contain much helpful data, but it does not follow that the image is somehow deficient. As repeatedly explained to counsel for the CTA by counsel for Mr. Pable, the fact that the CTA wiped the work profile installed on Mr. Pable's phone rendered much if not all relevant data inaccessible. The CTA's examination of the image confirms this, but the CTA provides no support for its further leap to the conclusion that Mr. Pable is nonetheless withholding relevant communications.[4]

[4] The declaration submitted by the CTA adds nothing to this argument. It says little more than, as expected, that the phone does not contain much data. What is more telling is what this declaration

Mr. Pable's expert was able to use the phone to access some of his communications on Google Hangouts (though not all that were accessible via a search of his Google account), and some of his communications via Signal, an application Mr. Pable used to send and receive, but not generally store, messages. This is not the same as accessing data stored in the physical device itself, and thus provides no basis on which to conclude there exists some trove of relevant messaging data on Mr. Pable's device that has not been produced. Equally misplaced is the CTA's complaint about "metadata" associated with these messages. Mr. Pable's Google Hangouts production was accompanied by detailed metadata associated with each message. There is no standard "native file" associated with a Signal message. And Mr. Pable has actually done more than was required by producing screen shots of his phone, which reproduce the messages as actually seen by him at the time as opposed to producing their content in some abstract electronic form. In any event, the CTA has identified no issue that turns on any metadata – there is no dispute as to the timing or provenance of any produced communication in this case.

At a minimum, the CTA should be required to explore these issue in depositions of Mr. Haynes and Mr. Pable before seeking the "extraordinary remedy" of another forensic examination of Mr. Pable's phone.

II. Mr. Pable Should Not Be Required to Produce "Archives" of His Personal Website.

There is not much to this issue. Mr. Pable has a personal website on which he mostly posts pictures of his dog, but also has references to his work for the CTA, much as any professional might discuss their work for a former employer.

---

does not say; namely, anything about the disabling of the work profile on the phone by the CTA, and why that does not explain the allegedly "missing" communications.

The CTA undertook to search Mr. Pable's public website, and apparently to search public Internet archives for prior versions of the website. It found material it has produced in the case (despite its irrelevance), and also found what it claimed was "proprietary" CTA code on the site. As explained above, this was code that Mr. Pable linked to on his site for the benefit of the CTA; indeed, the CTA was required to make it publicly available and Mr. Pable undertook to do that himself as there were no CTA resources available for such posting. Counsel for the CTA requested Mr. Pable take down the code, and he did. If there is any issue here, the CTA has all the relevant information. The further request for "archives" of Mr. Pable's website is a classic fishing expedition, and in any event a theoretical one since Mr. Pable has no such archive.

CONCLUSION

Mr. Pable respectfully requests that the Court deny the CTA's motion to compel production of his cell phone and website "archives."

February 12, 2020

Respectfully submitted,

/s/ Timothy A. Duffy
Timothy A. Duffy (ARDC #6224836)
Law Office of Timothy A. Duffy, P.C.
725 W Orchard Cir
Lake Forest, IL 60045
847-530-4920
tduffy@tduffylaw.com

Attorney for Plaintiff
Christopher George Pable